IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter (*underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of ensuring the security of a computer system comprising a host facility and a portable computing device coupled to the host facility, comprising the steps of:

loading software suitable for operating on the computer system in a secure environment on the computer system comprising the host facility and the portable computing device;

~~prior to operating~~ upon loading the software on the computer system, validating said software by the use of a validator program residing in the computer system in a secure fashion such that the validator program scans the software that is loaded in the secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking said software that is loaded as valid or invalid by the use of a ~~digital signature~~ flag; and,

denying said software the ability to operate on any environment within said computer system if said validator fails to identify said software as valid in order to ensure the security of said computer system.

2. (Original) The method described in Claim 1 wherein said method operates on an open platform computer system.

3. Canceled.

4. (Original) The method described in Claim 1 wherein said software is supplied by a third-party source.

5. (Original) The method described in Claim 4 wherein said third-party software is for execution or other use on a palmtop computer.

6. (Previously Presented) The method described in Claim 1 wherein said validator program is specially constructed to reside in a secure fashion in the host facility of said computer system.

7. (Currently Amended) The method described in Claim 1 wherein said method operates on a computer system which comprises:

a host computer; and

a portable computing device coupled to said host computer and wherein the validating operation is performed by the host computer for the portable computing device.

8. (Currently Amended) An apparatus for ensuring the security of a computer system, comprising:

a portable computing device coupled to a host computer, wherein said portable computing device is configured to load software from said host computer to said portable computing device for operating on said portable computing device; and,

a validation program residing on the computer system in a secure fashion that is configured for:

validating said software by first scanning said software that is loaded in a secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking said software as valid or invalid by the use of a ~~digital signature~~ flag; and,

denying said software the ability to operate in any environment on said computer system if said validator fails to identify said software as valid in order to ensure the security of said computer system.

9. (Original) The apparatus described in Claim 8 wherein said host computer is coupled to a network.

10. (Previously Presented) The apparatus described in Claim 8 wherein said portable computing device is a handheld computing device.

11. (Original) The apparatus described in Claim 8 wherein said portable computing device is a personal data assistant.

12. (Original) The apparatus described in Claim 8 wherein said portable computing device is coupled to said host computer by an infrared device.

13. (Original) The apparatus described in Claim 8 wherein said portable computing device is coupled to said host computer by an RF enabled device

14. (Previously Presented) The apparatus described in Claim 8 wherein said validation program resides in said host computer of the computer system in a fashion intended to be secure.

15. (Original) The apparatus described in Claim 8 wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software in said third-party software is not found to be clean of known security compromising routines.

16. (Previously Presented) The apparatus described in Claim 15 wherein said portable computing device is configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached..

17. (Previously Presented) The apparatus described in Claim 15 wherein said portable computing device is a Personal Data Assistant.

18. (Currently Amended) An apparatus for ensuring the security of a computer system, comprising:

a handheld computing device coupled to a network, wherein said handheld computing device is configured to load software from said network to said handheld computing device for operation on said handheld computing device; and,

a validation program that resides on the network that is configured for:

validating said software by scanning the files of said software in a secure environment on the handheld computing device ~~prior to operating~~ upon loading the software in any environment on the handheld computing device;

wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking said software as valid or invalid by the use of a ~~digital signature~~ flag; and,

denying said software the ability to operate on any environment on said computer system if said validator fails to identify said software as valid in order to ensure the security of said computer system.

19. (Previously Presented) The apparatus described in Claim 18 wherein said validation program resides in said network in a fashion intended to be secure.

20. (Previously Presented) The apparatus described in Claim 18, wherein said handheld computing device is configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached.

21. (Original) The apparatus described in Claim 18 wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software in said third-party software is not found to be clean of known security compromising routines.

22. (Withdrawn) A portable computing device, comprising:

a bus;

a processor coupled to said bus;

volatile RAM coupled to said bus;

non-volatile ROM coupled to said bus;

a data storage device coupled to said bud;

an operating system, capable of storage on said data storage device or said non-volatile ROM or both and capable of special configuration;

a display coupled to said bus;

an alpha-numeric input device coupled to said bus; and,

a cursor control device coupled to said bus;

all of which are capable of operating under the control of said operating system software or firmware.

23. (Withdrawn) The portable computing device described in Claim 22 wherein said portable computing device is a palmtop computing device.

24. (Withdrawn) The portable computing device described in Claim 22 wherein said portable computing device is a personal data assistant.

25. (Withdrawn) The portable computing device described in Claim 22 wherein said portable computing device is capable of coupling with a host computer.

26. (Withdrawn) The portable computing device described in Claim 22 wherein said operating system is configured to load third-party applications and other files if said applications and other files are flagged by a validation program as being clean of security compromising routines.

27. (Withdrawn) The portable computing device described in Claim 25 wherein said coupling is enabled by an infrared device.

28. (Withdrawn) The portable computing device described in Claim 25 wherein said coupling is enabled by an RF device.